bitwarden | Article du Centre d'Aide

SECRETS MANAGER > INTÉGRATIONS

Actions GitHub

Afficher dans le centre d'aide:
https://bitwarden.com/help/github-actions-integration/

Actions GitHub

Bitwarden fournit une intégration avec GitHub Actions pour récupérer les secrets de Secrets Manager et les injecter dans les workflows de GitHub Actions. L'intégration injectera les secrets récupérés sous forme de variables d'environnement masquées à l'intérieur d'une action. Pour configurer l'intégration:

Enregistrer un jeton d'accès

Dans cette étape, nous allons enregistrer un jeton d'accès en tant que secret crypté GitHub. Des secrets cryptés peuvent être créés pour une organisation, un dépôt ou un environnement de dépôt et sont mis à disposition pour être utilisés dans les workflows GitHub Actions :

1. Dans GitHub, naviguez jusqu'à votre dépôt et sélectionnez l'**onglet Paramètres**.
2. Dans la section Sécurité de la navigation à gauche, sélectionnez **Secrets et variables** → **Actions.**
3. Ouvrez l'onglet **Secrets** et sélectionnez le bouton **Nouveau secret de dépôt** .
4. Dans un autre onglet, ouvrez le coffre web de Secrets Manager et créez un jeton d'accès.
5. De retour sur GitHub, donnez à votre secret un **Nom** comme `BW_ACCESS_TOKEN` et collez la valeur du jeton d'accès de l'étape 4 dans l'entrée **Secret**.
6. Sélectionnez le bouton **Ajouter un secret**.

Ajoutez à votre fichier de flux de travail

Ensuite, nous allons ajouter quelques étapes à votre fichier de workflow GitHub Actions.

Obtenir des secrets

Pour obtenir des secrets dans votre flux de travail, ajoutez une étape avec les informations suivantes à votre fichier YAML de flux de travail :

```bash
- name: Get Secrets
  uses: bitwarden/sm-action@v2
  with:
    access_token: ${{ secrets.BW_ACCESS_TOKEN }}
    base_url: https://vault.bitwarden.com
    secrets: |
      fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff > SECRET_NAME_1
      bdbb16bc-0b9b-472e-99fa-af4101309076 > SECRET_NAME_2
```

Où :

- `${{ secrets.BW_ACCESS_TOKEN }}` fait référence à votre secret de dépôt précédemment enregistré. Changez en conséquence si vous n'avez pas nommé le secret `BW_ACCESS_TOKEN`.

- `fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff` et `bdbb16bc-0b9b-472e-99fa-af4101309076` sont des identifiants de référence pour les secrets stockés dans Secrets Manager. Le compte de service auquel appartient votre jeton d'accès **doit pouvoir accéder à ces secrets spécifiques**.

- `SECRET_NAME_1` et `SECRET_NAME_2` sont les noms que vous utiliserez pour référencer les valeurs secrètes injectées à l'étape suivante.

Utilisez des secrets

Enfin, vous pouvez compléter le chemin en référençant les noms secrets spécifiés (`SECRET_NAME_1` et `SECRET_NAME_2`) en tant que paramètres dans une action ultérieure, par exemple :

```bash
- name: Use Secret
  run: SQLCMD -S MYSQLSERVER -U "$SECRET_NAME_1" -P "$SECRET_NAME_2"
```